

[520.1007]

Abstract

The inventive method is based on a publicly known mathematical number group (G) and a higher order element of the group $g \in G$. In the first work step, a message corresponding to $N_i = g^{z_i} \bmod p$ is sent by each subscriber (T_i) to all other subscribers (T_j), (z_i) being a random number chosen from the set $(1, \dots, p-2)$ by a random number generator. In the second work step, each subscriber (T_i) selects a transmission key $k_{ij} = (g^{z_j})^{z_i}$ for each other subscriber (T_j) from the received message (g^{z_j}), with $i \neq j$, for transmitting their random number (z_i) to the subscribers (T_j). In the third work step, the common key k is calculated as $k = f(z_1, z_2, \dots, z_n)$ for each subscriber T_i . The inventive method can be advantageously used for generating a cryptographic key for a group of at least three subscribers.